COPY

Application No. 09,787,065
Art Unit No. 2135

REMARKS

This Amendment and Response is being submitted in response to the non-final Office Action mailed December 1, 2004. Claims 1-12, and 16-18 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney et al. (U.S. Pat. No. 6,351,813 B1). Claims 13-15 stand rejected over Mooney et al. (U.S. Pat. No. 6,351,813 B1) in view of Walsh et al. (U.S. Pat. No. 6,144,848).

In light of these rejections, the Applicant offers the following remarks.

CLAIM REJECTIONS

35 U.S.C. 103(a) – Mooney et al.

Claims 1-12, and 16-18 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney et al. (U.S. Pat. No. 6,351,813 B1).

Based on the Examiner's response, the Applicant respectfully submits that the Examiner has not yet fully understood the present invention. The inventive device is a device for supplying output data in reaction to input data. Such a device can, for example, be a smart card, which operates in an electronic door lock as it is, for example, outlined in column 8, lines 30-35, of Mooney et al. However, the claimed device has several distinctive features that are not disclosed by Mooney et al.

According to Mooney et al., when the user inserts her or his card into a card reader of the automatic door, the card reader sends a challenge message to the smart card, which corresponds to the device as mentioned in the first paragraph of claim 1. Then, the smart card encrypts this challenge message using a key stored in the smart card. The encrypted challenge message is the digital signature as mentioned in column 8, line 31, of document D1. The card reader itself may compare this digital signature to a set of pre-stored digital signatures to check whether the smart card supplying the digital signature is

8

allowed to enter the door or not. When the digital signature of the smart card in the card reader corresponds to a pre-stored digital signature the door is opened. When such a correspondence is not found, the door is not opened.

Mooney et al. describes only a smart card having an electronic circuit for executing an algorithm that generates the output data on the basis of the input data. The present invented smart card further includes the unit for detecting operational data as defined in the penultimate paragraph of claim 1, wherein the operational data detection unit is coupled to the electronic circuit as defined in the last paragraph of claim 1. Furthermore, Mooney et al. do not show the third and the fourth paragraphs of claim 1.

Every electronic circuit executing an algorithm provides operational data. The operation of the electronic circuit influences the operational data when the electronic circuit executes the algorithm. The operational data depend on the input data for the algorithm. Such operational data are, for example, a time needed by the electronic circuit to perform the algorithm or an electrical power consumed by the electronic circuit for executing the algorithm or an emitted electromagnetic radiation, or a snapshot of internal register states etc.

As defined in the penultimate paragraph of claim 1, the operational data are data which depend on the input data. Thus, the unit for detecting operational data of the electronic circuit as defined in the penultimate paragraph of claim 1 does not detect any data which has anything to do with the smart card, but is clearly limited to a unit which detects operational data, i.e. operational data of the electronic circuit which are influenced by an operation of the electronic circuit when the electronic circuit executes the algorithm wherein, importantly, the operational data depend on the input data.

The last paragraph of claim 1 specifies a very specific coupling between the operational data detection unit and the electronic circuit. This coupling is performed such that the operational data of the electronic circuit are used by the algorithm, which is executed by said electronic circuit for generating the output data. The immediate result

9

COPY

of this coupling of operational data into the electronic circuit is that the algorithm executed by the device is made hardware-dependent.

Regarding the unit for detecting operational data, the Examiner refers to column 2, lines 36-41. Possibly, the Examiner feels that "communication means" or the "automatic selection of appropriate communications for a particular (pair) of smart card reader and smart card" is related to the unit for detecting operational data. However, the communication means is only a feature of the access control/cryptosystem, but is not a feature of the smart card itself, i.e. the device for supplying output data in reaction to input data.

Should the Examiner feel that any data selecting appropriate communications might be "operational data", (although the Examiner does not argue in that way), the Applicant respectfully points out that data on the type of particular smart card reader and smart card are not "operational data, which depend on the input data". Data on the type of certain smart card or a certain smart card reader are static data, which are always the same irrespective of any input data. However, the operational data as defined in the third paragraph of claim 1 depend on the input data. Mooney et al. do not show this feature in column 2 or any other place.

If the digital signature mentioned in Mooney et al., column 8, line 31, depended on any operational data of smart card, which depend on the input data, i.e. a power measure, a time measure, etc., the complete system in document D1 would fail, since a "correct signature" could no longer be generated.

Regarding the last paragraph of claim 1, the Examiner points to Mooney et al., column 3, lines 30-46. The Applicant respectfully disagrees with the Examiner's analysis. Nowhere in the cited passage are any operational data detected by a certain operational detection unit coupled into the electronic circuit, i.e., as used by the algorithm for generating output data. Column 3 of Mooney et al. simply states that there are several

10

ways to handle encrypted files. There is no indication of operational data to be coupled into an algorithm executed by the electronic circuit.

The Examiner recites the passage "whereby the authenticity of the device is determined on the basis of the output data", although this text passage is not included in the presently pending documents. Additionally, the reference numbers cited by the Examiner on page 2 of the Office Action are also not included in the presently pending claims.

Claim 1 is not anticipated or rendered obvious by Mooney et al., since Mooney et al. only teach to use a normal smart card/smart card reader system, in which the output data only depends on the input data and an associated key, but does not depend on any operational data which depend on the input data.

In accordance with the present invention, the inventive smart card can, of course, be used as a smart card for a door lock system as mentioned in the specification. However, such a system in accordance with the present invention requires two similar smart cards, one smart card to be inserted into the door lock, and the other smart card being fixedly installed into the card reader, wherein both smart cards are provided with a challenge message, and the responses by both smart cards are compared to each other as defined in claim 17 or as illustrated in Fig. 4 of the application as filed.

Therefore, the subject matter of the present invention cannot be rendered obvious by Mooney et al. Causing the digital signature of Mooney et al. to depend on any operational data of smart card, which depend on the input data, i.e., a power measure, a time measure, etc., would cause the whole Mooney et al. system to fail, since a "correct signature" could no longer be generated.

Regarding claim 2, the Examiner points to Mooney et al., column 8, lines 47-52 and 62-64. The Examiner feels that any key attributes such as "life-span" and "security levels" of the keys have some relation to time data. However, the time data, as defined in

11

COPY

claim 2, is time the electronic circuit needs for executing the algorithm. Naturally, an algorithm execution time is dependent on input data. Therefore, claim 2 is only related to time data which are dependent on the input data. The life-span of a key or the security levels of keys, as disclosed by Mooney et al., are static data which are not dependent on any input data. Furthermore, the Applicant respectfully points out that an automatic selection of appropriate communications which are performed from outside a smart card, do not have to have anything to do with any life-spans or security levels of keys which are stored within the smart card.

Regarding claim 3, the Examiner points to column 6, lines 45-49. This text passage only states that there is a smart card 1190, which has stored on it a certain key. However, any "detection unit for detecting the operational data" is not mentioned in that place. Again, the Examiner is in contradiction to his assertion with respect to the detection unit in claim 1, since the text passage on claim 6 is completely free of any indication of any automatic communication selection, which is also not included in the smart card, but which is separated from the smart card as can be seen by the blocks 860, 870, 880, 890, which are clearly separate from the card which is illustrated to the right of the last line of Fig. 8.

Regarding claim 5, the Examiner points to column 3, lines 61-67. Possibly, the Examiner compares the "special generation function" or any "special security program" to the "cryptoalgorithm". However, any operational data detection regarding the selection of an automatic communication protocol as outlined in the Office Action on page 2, column 2, lines 36-41, does not have any relation to security program or the key generation function. The same is true for column 4, lines 1-4, where an access to the smart card is mentioned.

Regarding claim 6, the passage cited by the Examiner does not disclose the detection of operational data depending on input data, i.e. the input data into the "cryptoalgorithm of claim 5" or the "check some algorithm" in claim 6.

COPY

Regarding claim 7, the Examiner does not state where any operational data of the electronic circuit performing the cryptoalgorithm, which depend on the input data, is used in the subsequent algorithm step. Mooney et al., column 3, lines 61-67, and column 4, lines 1-4, do not show any multi-step algorithm.

Regarding claim 8, the Examiner points to column 8, lines 62-67. However, the stopping of the operation of the electronic circuit after a predetermined execution time during execution does not have anything to do with a life-span, since execution of the algorithm is continued, but not with the operational data. Furthermore, it would not make any sense to feed anything into an algorithm when the life-span of a circuit has expired. Then, one would not feed anything anywhere, since, after expiration of the life-span, a device is thrown away.

Regarding claim 9, the Examiner points to column 3, lines 64-67. This passage does not include any hint to any operational data, i.e. operational data of the electronic circuit which are influenced by an operation of the electronic circuit and which depend on the input data. Instead, a pseudo-random key generator only generates a pseudo-random number, which is then used to generate a key. No operational data during this process are fed into the key generator, since this would destroy the output of the key generator completely.

Regarding claim 10, the Examiner refers to column 3, lines 30-46. From this citation, I have the impression that the Examiner feels that the operational data as defined in claim 1 are encrypted files. This is, however, in clear contradiction to the Examiner's statements with respect to claim 1, where the operational data do have something to do with an automatic selection of communication protocols. Naturally, the encrypted data corresponds to the output data so that the operational-data, which depend on the input data, cannot be an encrypted output. Furthermore, an encrypted output is not an "operational data of an electronic circuit, which are influenced by an operation of the electronic circuit as defined in the third paragraph of claim 1". It is the very key feature

COPY

of encryption that encrypted output data only depend on the key and on the input, but not on any operational data or hardware features.

Regarding claim 11, the Examiner outlines several passages in document D1. However, the Examiner is again in clear contradiction to the "operational data", as asserted by the Examiner with respect to claim 1. Furthermore, I cannot see from the cited passages, where, as defined in claim 11, there is a test algorithm, and where there is a cryptoalgorithm, or a check sum algorithm, wherein the operational data of the test algorithm are processed in the cryptoalgorithm.

Regarding claim 12, the Examiner points to column 5, lines 22-40; however, only the DES algorithm is illustrated there. Further, this passage does not show that a test algorithm is performed in the first sub-circuit, while the DES algorithm is performed in the second sub-circuit. The cited passage only recites a single DES key to be stored on a smart card. Importantly, this passage does not even show any carrying out of the DES algorithm and, therefore, also does not show the further limitations of claim 12.

Regarding independent claim 17, the same arguments as brought forward with respect to claim 1 apply. Furthermore, claim 17 defines the parallel operation of the device to be tested and the examination device, while at the end of this procedure the output data from the device to be tested is compared to the output data of the examination device for subsequently affirming the authenticity. Importantly, the same information is input into both devices. However, in column 7, lines 6-9, only a single user input is shown, which results in an unlock of a security compartment of the smart card. Regarding feeding the input data into the examination device, the Examiner refers to column 4, lines 2-4. However, the Examiner obviously ignored the fact that the devices are different from each other, although column 4, lines 2-4, relates to the same smart card as mentioned in column 7.

Regarding the comparing step, claim 17 requires that the output data of the device to be tested is compared to the output data of the examination device. The Examiner

14

cites column 5, lines 36-45. However, this passage is completely silent on any comparison. Nothing like that is shown in column 5, lines 36-45.

Similarly, the Examiner's citation relevant to claim 18 does not correspond to the claimed language. Regarding the "feeding step", the Examiner refers to column 5, lines 45-47. However, this passage does not disclose any indication that the device is a device which is instructed as defined in claim 1, as has been outlined above with respect to claim 1. Furthermore, the generating step for generating the output data, in response to the random word as the input data, is not disclosed by Mooney et al. since no operational data of the electronic circuit processing the random word are measured and used by the algorithm for generating the output data as the key. The same arguments apply for the feeding step and for the generating step with respect to the second device.

In light of the comments presented herein, the Applicant submits that claims 1-12, and 16-18 are indeed novel over Mooney et al. (U.S. Pat. No. 6,351,813 B1). Applicant respectfully requests the withdrawal of the current rejection, and submits that the claims are in condition for allowance.

35 U.S.C. 103(a) – Mooney et al.

Claims 13-15 stand rejected over Mooney et al. (U.S. Pat. No. 6,351,813 B1) in view of Walsh et al. (U.S. Pat. No. 6,144,848). Again, the Applicant respectfully submits that the Examiner has not fully grasped the present invention as defined by the claims.

Regarding claim 13, the Examiner refers to claim 32 of Walsh et al. This claim, however, relates to a device for measuring the amount of energy stored in a power source. This power source is a battery or a capacitor as outlined in claim 30. Naturally measuring a power in a battery or capacitor has nothing to do with any operational data of an electronic circuit performing a certain algorithm. By measuring the power in a power source, one cannot come to a measurement of a power consumed by a certain task,

wherein this task is, importantly, the generation of the output data in response to the input data.

Regarding claim 14, the Examiner refers to claim 33 of Walsh et al. Respectfully, the Applicant submits that there is no resistor, a capacitor, or analog-digital converter in claim 33. Walsh's claim relates only to the power source rather than a measurement apparatus, as required by Applicant's claim 14.

Regarding claim 15, Walsh does not mention an internal clock generator in the cited passage, wherein "internal" is related to the device, which would mean in the terms of Mooney et al., within the smart card.

In light of the comments presented herein, the Applicant submits that claims 13-15 are indeed novel over Mooney et al. (U.S. Pat. No. 6,351,813 B1) in view of Walsh et al. (U.S. Pat. No. 6,144,848). Applicant respectfully requests the withdrawal of the current rejection, and submits that the claims are in condition for allowance.
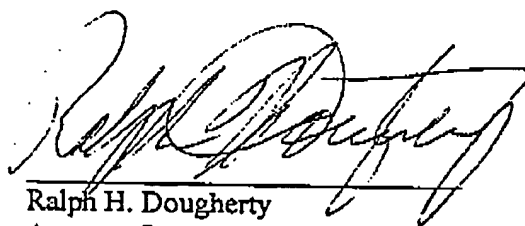
16

RECEIVED
CENTRAL FAX CENTER

JUL 1 0 2006

Application No. 09,787,065
Art Unit No. 2135

REMARKS

Respectfully submitted,

Ralph H. Dougherty
Attorney for Applicant(s)
Registration No. 25,851
DOUGHERTY CLEMENTS
1901 Roxborough Road, Suite 300
Charlotte, North Carolina 28211 USA
Telephone: 704.366.6642
Facsimile: 704.366.9744
rdougherty@worldpatents.com

RHD/BGW/bcb

17